TARDEC

---TECHNICAL REPORT---

THE NATION'S LABORATORY FOR ADVANCED AUTOMOTIVE TECHNOLOGY

No. 13756

1995 Presidential Award for Quality
TARDEC

RIDE MOTION SIMULATOR
SAFETY ASSESSMENT REPORT

December 1, 1998

By MTS Systems Corporation
1400 Technology Drive
Eden Prairie, MN 55344

APPROVED FOR PUBLIC RELEASE
DISTRIBUTION UNLIMITED

WINNER OF THE 1995 PRESIDENTIAL AWARD FOR QUALITY

U.S. Army Tank-Automotive Research,
Development, and Engineering Center
Detroit Arsenal
Warren, Michigan 48397-5000

NOTICES

This report is not to be construed as an official Department of the Army position.

Mention of any trade names or manufacturers in this report shall not be construed as an official endorsement of approval of such products or companies by the U.S. Government.

Destroy report when it is no longer needed. Do not return it to the originator.

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1, 1998	Final, March - December 1998

4. TITLE AND SUBTITLE
Ride Motion Simulator Safety Assessment Report

5. FUNDING NUMBERS

6. AUTHOR(S)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
MTS Systems Corporation
14000 Technology Drive
Eden Prairie, MN 55344

8. PERFORMING ORGANIZATION REPORT NUMBER
13756

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
See distribution page

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*
This report documents the analysis of the Ride Motion Simulator (RMS) designed for the U.S. Army Tank-automotive and Armaments Command (TACOM) in Warren, Michigan. It provides system and component descriptions and a specific hazard analysis of the RMS. The scope of this analysis is the systematic assessment of the real and potential hazards associated with the RMS. This report is an attempt to identify hazards and to discuss the elimination or control of the identified hazards. This documentation is used to assist TACOM in obtaining a man-rating status for the RMS.

14. SUBJECT TERMS
humans RMS ride motion simulator man-rated simulation vibration safety assessment hazard analysis

15. NUMBER OF PAGES
45

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNL

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The Report Documentation Page (RDP) is used in announcing and cataloging reports. It is important that this information be consistent with the rest of the report, particularly the cover and title page. Instructions for filling in each block of the form follow. It is important to ***stay within the lines*** to meet ***optical scanning requirements.***

Block 1. Agency Use Only *(Leave blank).*

Block 2. Report Date. Full publication date including day, month, and year, if available
(e.g. 1 Jan 88). Must cite at least the year.

Block 3. Type of Report and Dates Covered. State whether report is interim, final, etc. If applicable, enter inclusive report dates (e.g. 10 Jun 87 - 30 Jun 88).

Block 4. Title and Subtitle. A title is taken from the part of the report that provides the most meaningful and complete information. When a report is prepared in more than one volume, repeat the primary title, add volume number, and include subtitle for the specific volume. On classified documents enter the title classification in parentheses.

Block 5. Funding Numbers. To include contract and grant numbers; may include program element number(s), project number(s), task number(s), and work unit number(s). Use the following labels:

C - Contract	**PR** - Project
G - Grant	**TA** - Task
PE - Program Element	**WU** - Work Unit Accession No.

Block 6. Author(s). Name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. If editor or compiler, this should follow the name(s).

Block 7. Performing Organization Name(s) and Address(es). Self-explanatory.

Block 8. Performing Organization Report Number. Enter the unique alphanumeric report number(s) assigned by the organization performing the report.

Block 9. Sponsoring/Monitoring Agency Name(s) and Address(es). Self-explanatory.

Block 10. Sponsoring/Monitoring Agency Report Number. *(If known)*

Block 11. Supplementary Notes. Enter information not included elsewhere such as: Prepared in cooperation with....; Trans. of....; To be published in.... When a report is revised, include a statement whether the new report supersedes or supplements the older report.

Block 12a. Distribution/Availability Statement. Denotes public availability or limitations. Cite any availability to the public. Enter additional limitations or special markings in all capitals (e.g. NOFORN, REL, ITAR).

DOD - See DoDD 5230.24, "Distribution Statements on Technical Documents."
DOE - See authorities.
NASA - See Handbook NHB 2200.2.
NTIS - Leave blank.

Block 12b. Distribution Code.

DOD - Leave blank.
DOE - Enter DOE distribution categories from the Standard Distribution for Unclassified Scientific and Technical Reports.
Leave blank.
NASA - Leave blank.
NTIS -

Block 13. Abstract. Include a brief *(Maximum 200 words)* factual summary of the most significant information contained in the report.

Block 14. Subject Terms. Keywords or phrases identifying major subjects in the report.

Block 15. Number of Pages. Enter the total number of pages.

Block 16. Price Code. Enter appropriate price code *(NTIS only).*

Blocks 17. - 19. Security Classifications. Self- explanatory. Enter U.S. Security Classification in accordance with U.S. Security Regulations (i.e., UNCLASSIFIED). If form contains classified information, stamp classification on the top and bottom of the page.

Block 20. Limitation of Abstract. This block must be completed to assign a limitation to the abstract. Enter either UL (unlimited) or SAR (same as report). An entry in this block is necessary if the abstract is to be limited. If blank, the abstract is assumed to be unlimited.

U.S. Army
Tank-automotive and Armaments Command

TARDEC PSL Upgrade

Contract Number:
DAAE07-95-C-X113

Ride Motion Simulator Safety Assessment Report

December 1, 1998

Prepared For:
Mr. Harry Zywiol
U.S. Army Tank-automotive and
Armaments Command
AMSTA-TR-D MS#157 Bldg#215
Warren, MI 48397-5000

Prepared By:
MTS Systems Corporation
14000 Technology Drive
Eden Prairie, MN 55344

Distribution:
J. Lenkeit, DRI
P. Furman, MTS

Table of Contents

List of Figures

1.0 INTRODUCTION

This report documents the analysis of the Ride Motion Simulator (RMS) designed for the United States Army Tank-automotive and Armaments Command (TACOM) in Warren, Michigan. It provides system and component descriptions and a specific hazard analysis of the RMS.

The scope of this analysis is the systematic assessment of the real and potential hazards associated with the Ride Motion Simulator. This report is an attempt to identify hazards and to discuss the elimination or control of the identified hazards.

2.0 OBJECTIVES

The primary goal is to provide documentation which assists the Tank-Automotive Research, Development and Engineering Center (TARDEC) in obtaining a man-rating status for the Ride Motion Simulator.

3.0 CONCLUSIONS

All known safety hazards have been evaluated throughout the analysis of the Ride Motion Simulator.

The design features and safety devices for the Ride Motion Simulator, when used in conjunction with test specific operating procedures, will reduce the probability of injury to occupant or damage to equipment.

4.0 RECOMMENDATIONS

Given the user interface flexibility and the large potential power of the RMS as dictated by the specification, we recommend that TARDEC develop a step-by-step checklist of safe operating procedures for each human subject test.

5.0 DISCUSSION

5.1 SYSTEM DESCRIPTION

The Ride Motion Simulator is based upon the Stewart platform style of motion platform design. This mechanism, also commonly referred to as a hexapod, uses six linear actuators to connect a triangular fixed base with a triangular motion platform. The six actuators, the base and the platform form a near octahedral structure. Through control of the six actuators, this mechanism provides for independent or simultaneous motion of the platform in the six natural degrees-of-freedom.

The RMS is composed of the following major subsystems:

- Cab
- Hexapod
- Hydraulic Supply and Distribution
- Electronic Controls
- Controller Software

Figures 5-1 through 5-3 are photographs of the RMS and associated equipment.

5.2 SYSTEM PERFORMANCE

The intended closed-loop performance of the RMS motion platform is summarized below:

- payload: 600 lb
- frequency response: -3db at 40 Hz
- performance capability per axis:

Axis	Displacement	Velocity	Acceleration
X (longitudinal)	± 20 in	± 30 in/s	± 1.0 g
Y (lateral)	± 20 in	± 30 in/s	± 1.0 g
Z (vertical)	± 20 in	± 50 in/s	± 2.0 g
Roll (about X)	± 20 °	± 70 °/s	± 1146 °/s^2
Pitch (about Y)	± 20 °	± 70 °/s	± 1146 °/s^2
Yaw (about Z)	± 20 °	± 90 °/s	± 1146 °/s^2

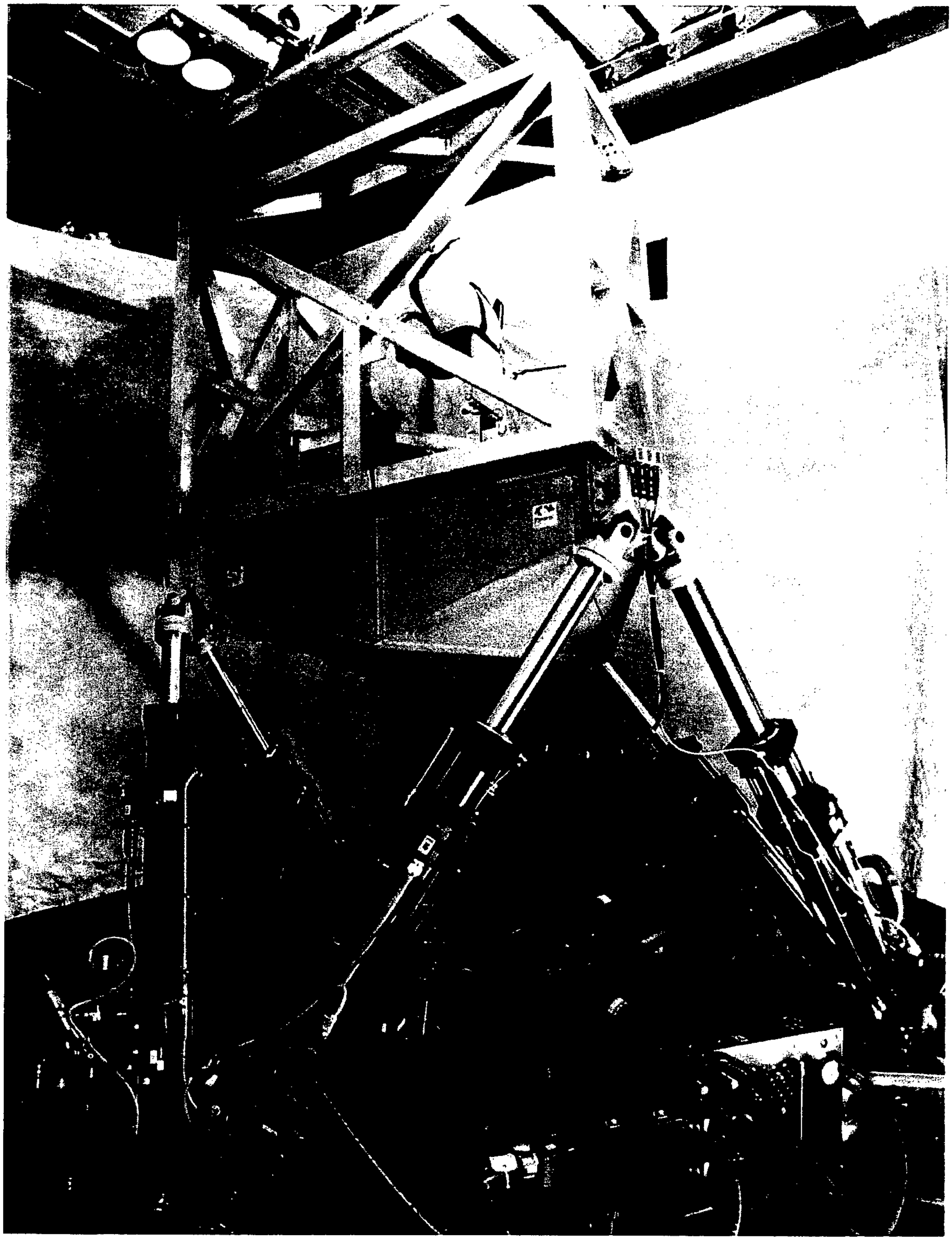

Figure 5-1. Ride Motion Simulator (front view)

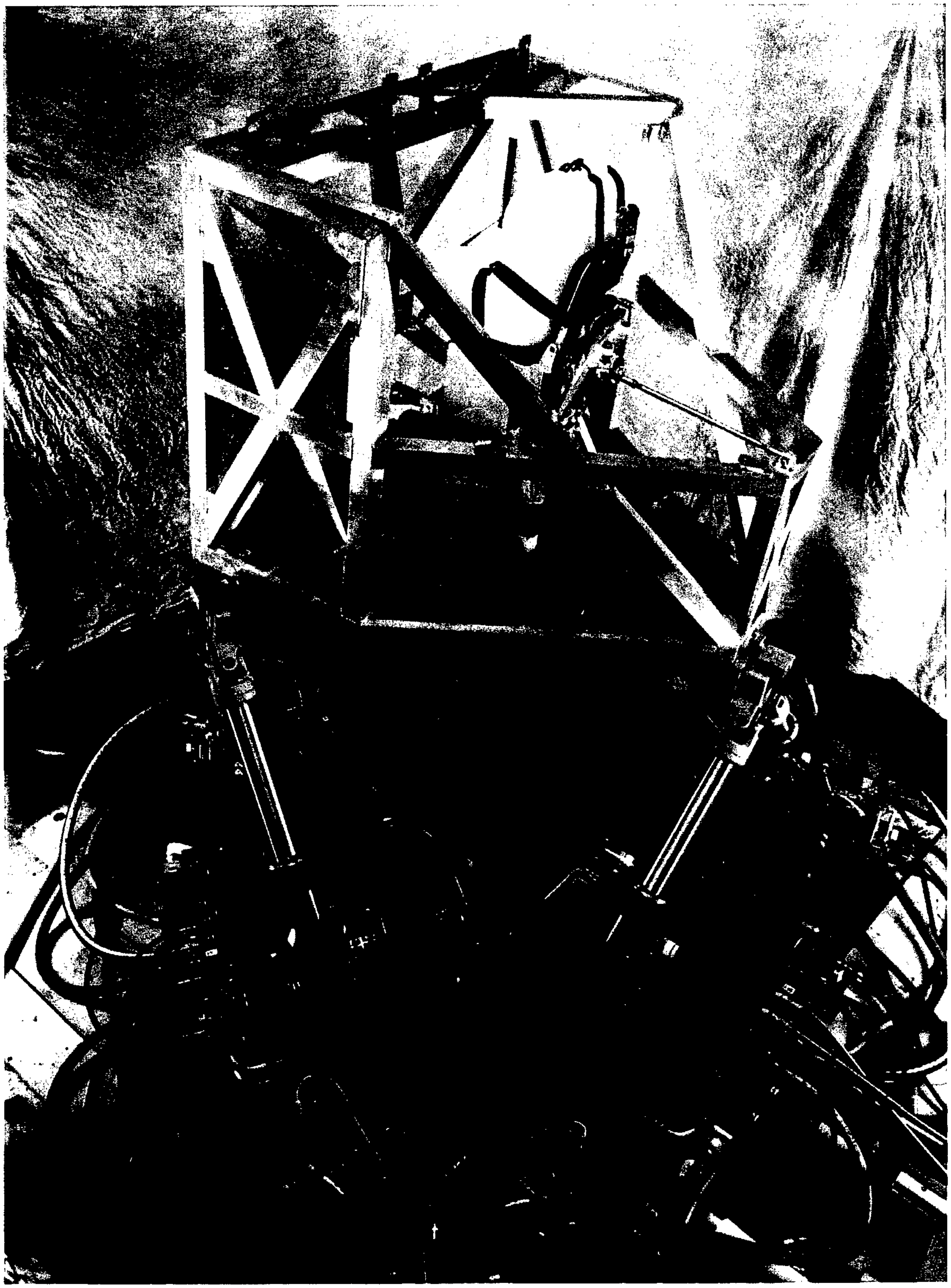

Figure 5-2. Ride Motion Simulator (top view)

Figure 5-3. RMS Electronic Controls

The following figures provide examples of the system performance.

Figure 5-4 is a plot of the transfer function between the Z-axis acceleration command and feedback showing the vibration capacity of the system.

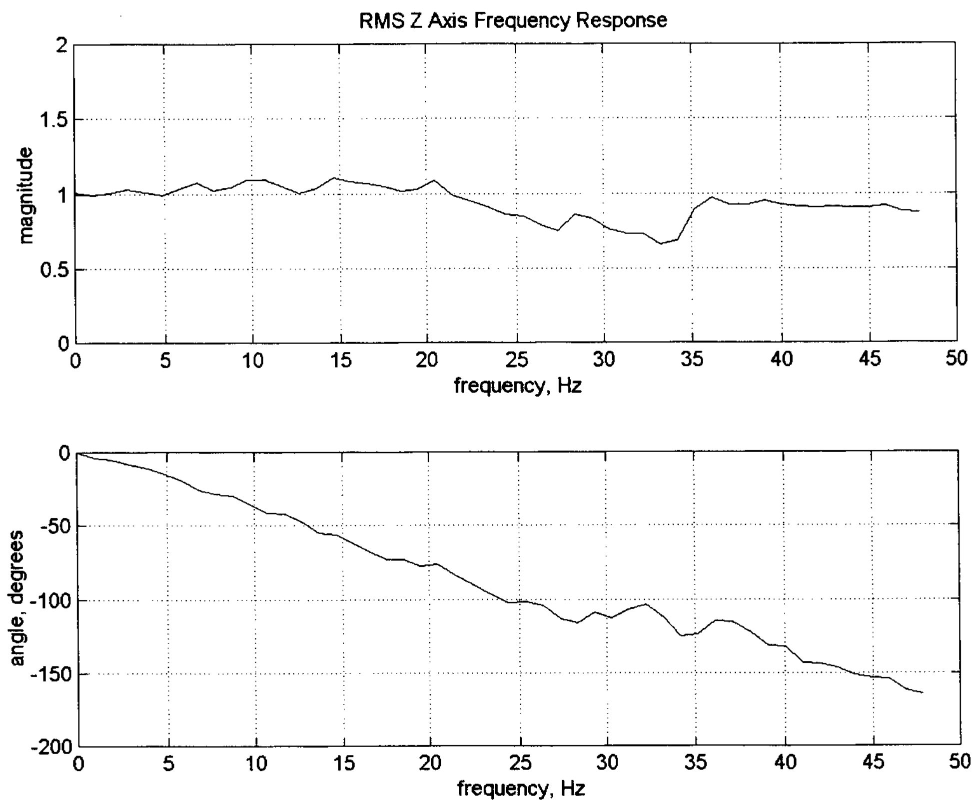

Figure 5-4. Z-axis Acceleration Transfer Function

Figure 5-5 shows a Z-axis time history following the Perryman2 test track data. The data was supplied by TARDEC and represents an M1 tank running at 23 mph on the Perryman2 test track. This data was high pass filtered using a 2-pole Butterworth filter with a break frequency of 1 Hz. The peak acceleration shown requires 80% of the rated flow on the valves.

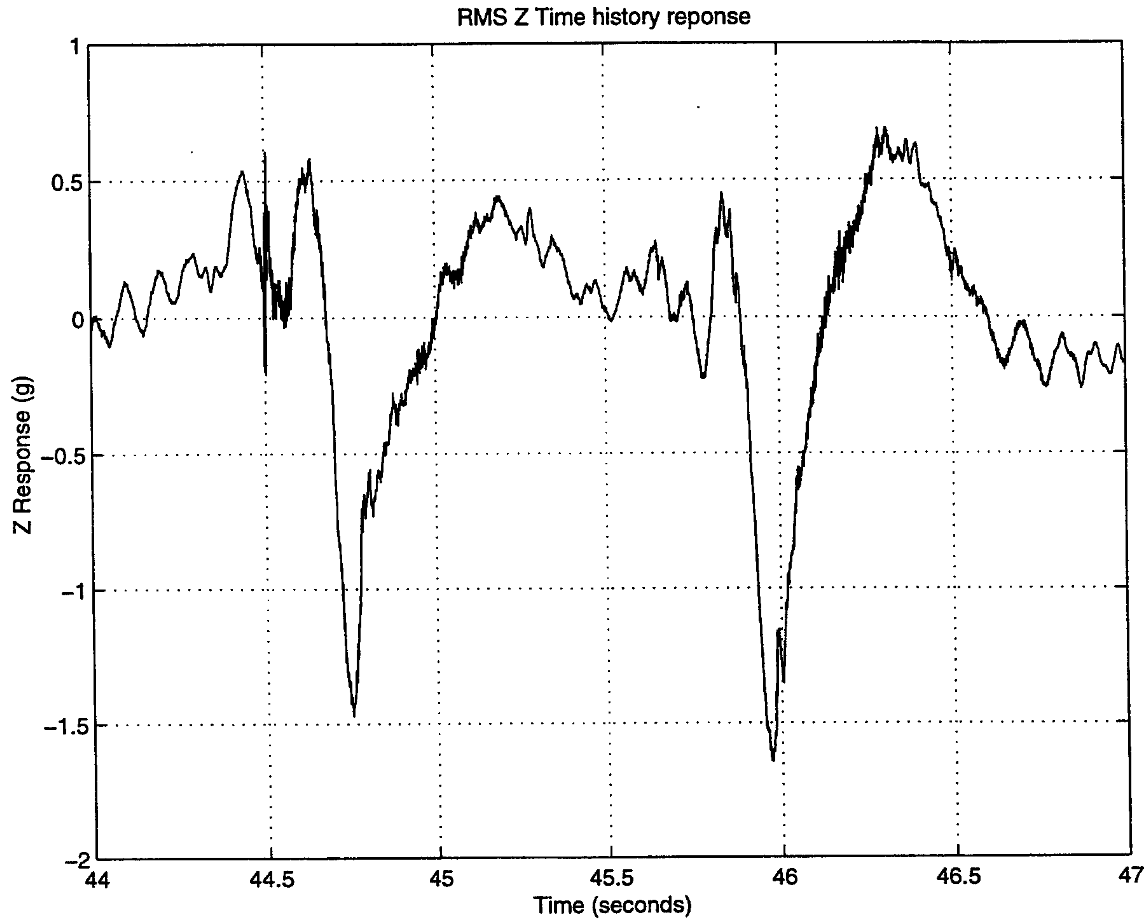

Figure 5-5. Z- Axis Time History

5.2.1 MAXIMUM SYSTEM ACCELERATION AND DECELERATION

A number of tests were performed on the RMS to experimentally verify the performance as well as document the maximum acceleration and deceleration capability for a nominally configured payload. These tests were conducted with all electronic and software safety features disabled. The recorded data is presented in the table below. Due to the number of degrees of freedom and high cross-coupling inherent with the hexapod, along with the flexibility allowed for both cab payload and controller, it cannot be stated that these maximums are absolute. It can be stated that the data presented below is a best account of the maximum acceleration and deceleration capacity of the RMS for the conditions of this test.

Motion	Acceleration	Deceleration
Along + Z axis into retract cushions	+ 10 g	- 10 g
Along - Z axis into retract cushions	- 8 g	+ 4 g
Along +X axis into actuator 1 & 6 cushions	+ 3 g	- 4 g
Along +X axis into actuator 2 & 5 cushions	+ 3 g	- 4 g
About +Y axis (pitching): • actuator 1, 2, 5 & 6 into extend cushions • actuator 3 & 4 into retract cushions	+2300 $^\circ/s^2$	- 5700 $^\circ/s^2$
Actuator 5 open-loop into retract cushion, all other actuators commanded to hold	max. translation: X = -3 g Max. rotation: roll = 1700 $^\circ/s^2$	max. translation: Z = - 4 g Max. rotation: roll = 2300 $^\circ/s^2$

An example of the test data from which the above table was generated is shown in Figure 5-6. For this experiment, the RMS was positioned at 10 inches above the home position for the start of the test. It was then given a position command of maximum acceleration to full velocity in the positive Z direction (downward) and along the vertical Z axis until all motion was fully arrested by the six actuator cushions. This data describes a worst case scenario because all six actuators maintain a driving force through the cushion, and all actuators enter their cushions almost simultaneously. The operating pressure for Figure 5-6 was 1,200 psi. However, during integration and tuning on site at TARDEC, the HPS pressure was adjusted to 600 psi. This was done to increase the safety while still meeting all system performance specifications. Therefore, the minimum and maximum acceleration and deceleration curve results in less severe motion.

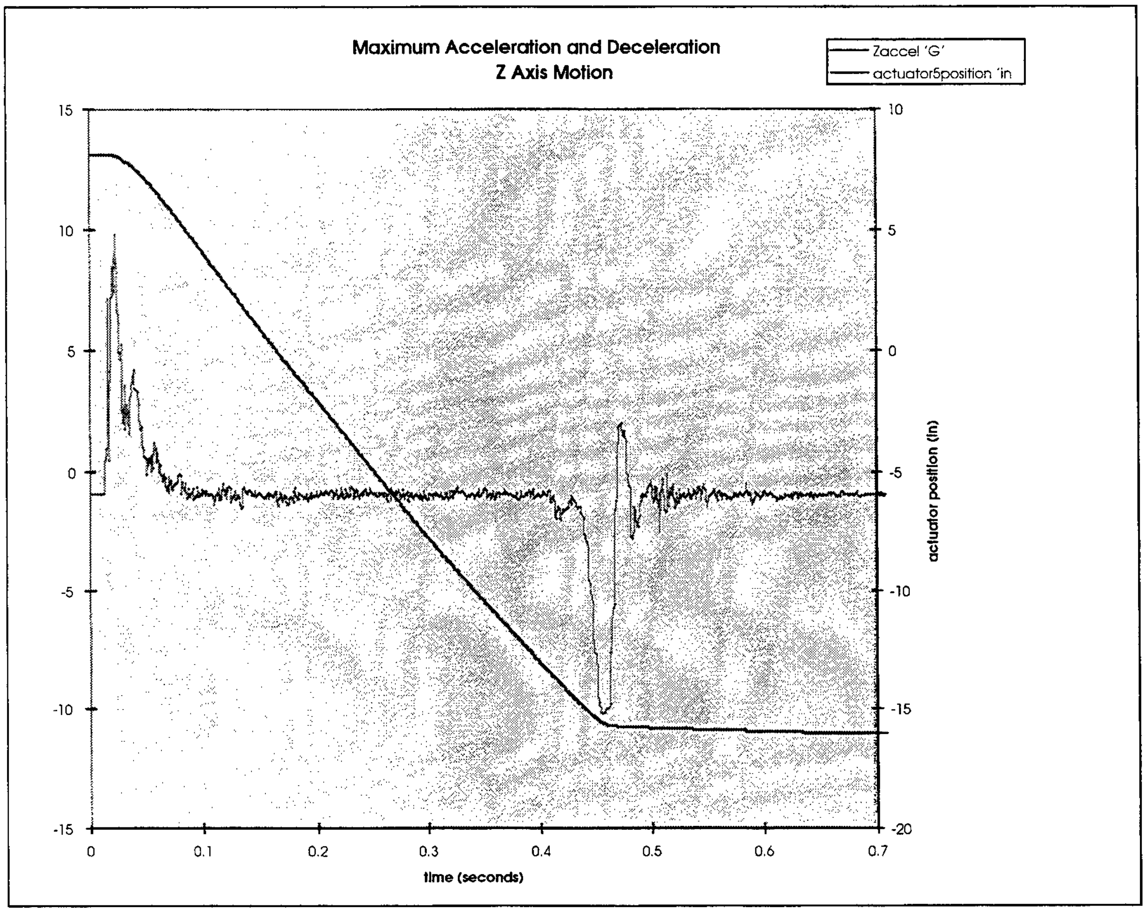

Figure 5-6. Maximum Acceleration and Deceleration - Z Axis Motion

5.3 RMS HAZARD EVALUATION

The analysis results presented on the following pages address the hazard potential to the Ride Motion Simulator should there be a failure in any of the RMS subsystems.

The hazard evaluation of the RMS is made with a higher degree of confidence than would be expected for an entirely new system. Starting with an analysis of the old RMS and CS/TMBS (Crew Station/Turret Motion Base Simulator) design, the reliable and safe features have been retained while safety improvements have been made to many areas.

The hazard assessment is divided into two parts as follows:

- A general safety analysis for each RMS subsystem (Section 5.4)

- An analysis of each possible hazard, failure probability and backup system presented in table format (Section 5.5)

5.4 SAFETY ANALYSIS OF EACH SUBSYSTEM

This section provides a safety analysis of each of the following RMS subsystems:

- Cab (Subsection 5.4.1)
- Hexapod (Subsection 5.4.2)
- Hydraulic Supply and Distribution (Subsection 5.4.3)
- Electronic Controls (Subsection 5.4.4)
- Controller Software (Subsection 5.4.5)

Each subsection provides a description of the subsystem, a structural integrity overview (if applicable), and an analysis of subsystem failures that may occur.

5.4.1 CAB SAFETY ANALYSIS

5.4.1.1 CAB DESCRIPTION

The cab was designed with the intent that it could be easily reconfigured to replicate a number of military vehicles, including but not limited to, automobiles, light and heavy trucks, tanks and other armored vehicles.

The cab is composed of the following mechanical components:

- Cab Frame
- Cab Attachment Fittings
- Seat Attachment Plate
- Miscellaneous equipment mounting hardware including seat support roads and fittings (as required) and attachment fitting for computer monitors, controls, display panels, etc. (as required).

Each of these components are described in the following sections.

5.4.1.1.1 CAB FRAME

The cab frame is a 3-dimensional welded space frame which forms the circumferential structure of the simulated crew compartment. The main function of the Cab Frame is to provide stiff structural attachment points for various components of the simulated crew compartment including the seat, controls, foot pedals, computer monitors, etc. The required components are mounted to the framework by means of appropriate brackets, subframes, and fastening techniques. The inertial loads generated by such mounted equipment, are transferred to the hexapod by the Cab Frame. The framework itself can be easily removed from the motion base to allow for maintenance or remote setup.

The Cab Frame structure is primarily fabricated from 3 inch square aluminum box beams (wall thickness = 0.125 inch) welded together to form a stiff 3-dimensional space frame.

Safety Features

The cab frame is primarily designed to meet the system minimum natural frequency criteria (a stiffness design rather than a strength design), therefore, the space frame is in general subjected

to low stresses even at maximum system accelerations. At the three cab to platform attachment points, the box beam wall thickness is increased to 0.25 inch to provide additional strength.

5.4.1.1.2 CAB ATTACHMENT FITTINGS

The cab frame with its triangular footprint is attached to the platform at the three platform corners. The attachment loads at these corners are transferred to the cab frame via three machined steel fittings which are bolted to the cab frame truss members with 16 bolts per fitting. The fittings are mounted inside of cab frame box beams and are therefore nearly invisible to the casual observer.

Safety Features

When the cab frame is placed on the platform or on the shop floor, it rests on the lower surface of the cab attachment fittings. The fittings are made of steel to minimize damage which might result when the cab is moved. If a fitting is damaged it may be removed from the assembly for repair or replacement.

5.4.1.1.3 SEAT ATTACHMENT PLATE

Various crew seats may be mounted to the simulator using structural attachment points which are unique for each configuration. In each case the bottom of the seat is attached to the seat attachment plate. In addition to the lower main attachment point, some seat configurations utilize upper support points to reduce the cantilevered moments transferred to the lower support point.

The seat attachment plate is located near the bottom center of the cab frame and serves as the main structural attachment point for the crew seat. The location and size of the plate was chosen to accommodate different seat mount locations for the M1 Gunner, M1 Commander, M1 Driver, Bradley Commander and Bradley Driver.

The seat attachment plate visually appears as if it is a part of the cab frame, however, it is directly attached to the MTS Platform and "floats" with respect to the cab frame. Lower seat support loads are therefore transferred directly to the MTS platform without first passing through the cab frame.

The seat attachment plate is machined from a 2 inch thick aluminum plate which can be drilled and threaded to accommodate the various seat attachment bolt patterns.

The primary safety feature of the seat attachment plate design is the short load path which results when the seat loads are applied to the plate and in a matter of inches are transferred to the platform. This "load in/load out" design reduces bending moments and stresses in the plate.

Other safety features include the use of redundant high strength bolts to attach the plate to the platform and designated bolt torques to reduce bolt fatigue load cycles and provide friction shear load transfer between the plate and the platform.

In addition to the above listed structural safety items, the plate was designed as a stand alone, easy to replace item which is not permanently welded or attached to either the cab or the platform. The expected use of the simulator presumes that the seat attachment plate will be removed, modified and reinstalled as the cab configurations are changed. This process increases

the risk that at some point in time the plate may be damaged. Therefore, the easy removal of the plate for replacement or repairs should reduce the temptation to use a "slightly damaged" plate.

5.4.1.1.4 SEAT SUPPORT RODS AND FITTINGS AND ATTACHMENT FITTINGS

Each simulated crew compartment assembly may involve the mounting of various pieces of auxiliary equipment such as display monitors, control pedals and yokes, instrument panels, and other pieces of equipment required to properly simulate the crew compartment. This type of equipment may be mounted to the cab frame using brackets and struts designed specifically for each simulated crew compartment.

Safety Features

In general these types of brackets and struts will be designed by the end user. The equipment delivered with the cab was designed to minimize bending moments when possible thereby reducing stresses and increasing the stiffness of the equipment mounts.

5.4.1.2 CAB STRUCTURAL INTEGRITY

The major load carrying elements of the cab assembly are the cab frame, seat attachment plate and the cab to platform attachment hardware. To reduce the risk of structural failures which could cause injury or damage to other simulator elements the following general design guidelines were followed:

- The design loads are based on maximum system accelerations which can be produced without considering mechanical or software safety functions.
- Structural safety factors on all parts are higher than the required value of 2.0 with the safety factor on major load carrying elements being 3.8 or higher.
- Ductile materials were used so that overload situations (if they occur) will initially bend or stretch structural elements rather than break them.
- Redundant load paths were used when possible.

The following table summarizes the safety factors and safety related design approach for the major load carrying elements of the cab assembly.

Structural Element	Safety Factor	Risk Mitigating Design Features
Cab Frame	4.9	- Redundant load paths - High S.F.
Cab Attachment Fittings and Fasteners	5.5	- High S.F. - Steel base material to reduce installation damage - Redundant bolt patterns - Removable if damaged
Cab Attachment Bolts	4.3	- High S.F. - High Strength Bolts
Seat Attachment Plate	3.8	- Removable if damaged - One piece construction
Seat Attachment Plate Bolts	5.8	- Redundant load path - Specified torques to reduce bolt bending and bolt fatigue

5.4.2 HEXAPOD SAFETY ANALYSIS

5.4.2.1 HEXAPOD DESCRIPTION

The hexapod is composed of the following mechanical components:

- hydraulic actuators and swivels
- actuator drain sump pump
- platform
- isolation mass

Each of these components are described in detail as follows.

Hydraulic Actuators and Swivels

The six hydraulic actuators are the active links, or legs, supporting the motion platform. The actuators are connected to the system at each end with a swivel. The base swivel attaches the fixed bottom end of the actuator to the isolation mass. The table swivel attaches the moving top end of the actuator to the motion platform. The swivels allow the actuator to rotate about the base and table without imposing constraint to motion. The actuator is composed of a piston/cylinder of equal acting area and a control manifold. The piston/cylinder incorporates hydrostatic bearings for low friction performance and hydraulic cushions to limit deceleration at the limits of stroke. The actuator control manifolds house safety and control devices for regulating pressure in the cylinder. The principle functions designed into actuator control manifolds are summarized below:

- three-stage servovalves provide regulation of hydraulic flow to the cylinder during normal operation
- blocking valves isolate the cylinder from the servovalve and main oil supply when electrical power is removed from the enable/abort solenoid valve
- pressure relief valves limit the maximum load pressure (delta-pressure) which can be applied to the actuator piston
- pairs of pressure relief valves are employed for redundancy
- pressure dump valves provide an escape path for cylinder pressure and an entrance path for retract accumulator oil; the dump valves operate in parallel with the blocking valves, they open when electrical power is removed from the enable/abort solenoid valve
- the settling orifice restricts the flow of oil out of the cylinder limiting platform velocity when the table moves to the park position after E-Stop

Safety Features

- a separate pilot supply for the three-stage servovalve and safety valves increases system predictability and safety during aggressive E-Stop shutdown events
- pilot controlled three-stage servovalves provide the second redundant means of isolating the main source of hydraulic power from the actuator
- solenoid controlled blocking valves provide the third redundant means of isolating the main source of hydraulic power from the actuator
- pressure relief valves limit maximum acceleration of the motion platform
- solenoid controlled pressure dump valves further attenuate platform acceleration after invoking an E-Stop
- actuator hydraulic cushions limit platform deceleration at the limits of stroke
- the abort/retract accumulator, pressure dump valve, and settling orifice function together to smoothly return the motion platform to the parked position after E-Stop or after hydraulic pressure is removed and the motion platform is not in the parked position
- pressure transducers allow software limits to be applied to the load pressure (delta-pressure) generated by each actuator and thus provide a redundant means of limiting maximum acceleration of the motion platform

Actuator Drain Sump Pump

The actuator drain sump pump provides a near zero back pressure drain system for the RMS actuators. Drain flow from the six actuators is directed to the sump reservoir located below floor level and directly below the center of the RMS. Float level switches detect oil level inside the reservoir and a motor/hydraulic pump unit built into the reservoir pumps oil back to the hydraulic service manifolds (HSM) where it joins return flow back to the hydraulic power unit (HPU).

Safety Features

- a flood level switch detects reservoir oil level above the normal high level sensor and is provided as an input to the controller; software limit configuration determines simulator response to a reservoir flood level condition

Platform

The triangular shaped platform is the moving structure to which actuator swivels and simulator cab are attached. The table is of all aluminum riveted construction in order to minimize mass and maximize stiffness and fatigue resistance.

Safety Features

- accelerometers attached to the platform allow software limits to be applied to each of the six degrees of world acceleration and thus provide further redundancy for detecting and limiting maximum acceleration of the motion platform

Isolation Mass

The isolation mass, to which the base of the RMS attaches serves to minimize the amount of vibration disturbance transmitted to the surrounding laboratory. The total weight of the isolation mass is approximately 230,000 lb. It is constructed of steel reinforced concrete and rests on compacted soil. Anchor plates and tie rods built into the structure provide the mechanical interface for the RMS actuator base swivels at the top surface of the isolation mass.

5.4.2.2 HEXAPOD STRUCTURAL INTEGRITY

The major load carrying elements of the RMS motion platform are the actuators, swivels, platform, and isolation mass. To mitigate risk of injury or damage to the simulator, the RMS employs three engineering approaches in the design of these structural elements:

- The first approach is to design structural elements such that stress level at maximum loading condition is not greater than 25% of the material ultimate strength. It is important to recognize that the maximum load for a given structural element is unique. It is a function of local sub-system structure and simulator attitude and acceleration.

- The second approach is to provide redundant load paths whenever possible, each of which is capable of handling the maximum loading condition. The riveted aluminum table is an excellent example of a structure which employs redundant load paths. Each joint of the table is composed of at least two structural elements which are connected by numerous rivets. In many cases, the table could easily survive maximum loading conditions even if 50% of the rivets were removed from the joint.

- The third approach employed is to neglect both mechanical and software acceleration limiting safety functions when computing maximum loading conditions for a given structural element. For example, the actuator pressure relief valves will limit the maximum vertical acceleration, but if the pressure relief valves are removed, the simulator is capable of accelerating at significantly higher rates.

Nevertheless, the RMS contains structural elements which in the event of failure could result in injury. The following table summarizes these critical, non-redundant load path, elements of the structure and describes the design approach employed to mitigate the risk of failure.

Subsystem	**Load Path Element**	**Risk Mitigating Design Features**
actuator	piston rod	• fatigue resistant base material • design safety factor >> 4
swivel		a prototype of the swivel design was built and the following design verification tests were performed prior to construction of the swivels installed on the RMS: • 10M cycle durability test, normal operating loads • 10K cycle durability test, maximum loads
	casting	• fatigue resistant base material • design safety factor >> 4 • complete X-ray inspection of every casting (ref. MIL STD 2175, Grade B, Class 1)
	pivot pins	• fatigue resistant base material • design safety factor >> 4 • redundant attachment fasteners
platform	seat attach plate	• high strength aluminum base material • monolithic construction • design safety factor >> 4 • near optimal attachment joint configuration
isolation mass	base swivel mount	• design safety factor >> 4

5.4.2.3 HYDRAULIC FAILURES RELATING TO THE HEXAPOD

Hose and Fitting Failure

The greatest hazard related to hydraulic power is the potential for a hose or fitting failure near the cab. The loss of control due to even a large hose failure is only a minor hazard. The major hazard is with the potential for discharging a large amount of hydraulic oil vapor into the laboratory environment. Also of concern is the possibility of imparting a dense cloud of high velocity oil vapor in the direction of the test subject or a nearby observer.

To mitigate the risk of hydraulic hose failure, RMS supply pressure hoses are rated for 3000 psi working pressure. Since the burst pressure of these hoses is 12,000 psi, a design safety factor of four, based on ultimate, is inherent in the hose working pressure rating. Since the RMS system pressure is 600 psi, this increases the inherent design safety factor of hoses by 5 times, raising the overall safety factor of RMS pressure hoses to 20. A parallel argument can be made regarding hydraulic fittings used on the RMS.

Subsystem Failure

Hydraulic pressure related failures are also a concern with the RMS HSM, actuator, and accumulator subsystems. Experience shows that catastrophic failure at the subsystem level is highly unlikely. The more likely scenario is a confined single component failure which results in loss of system performance and/or a quantity of oil being discharged into the environment. An example of such a failure would be a blown actuator seal or a crack developing in a manifold. In both of these cases, the resulting oil leak would become apparent either during simulator operation or upon pre-operating inspection.

To mitigate the risk of subsystem hydraulic failure, additional safety factors were engineered into components and proof pressure testing was conducted for each sub-assembly. For example, all accumulators installed on the RMS are fatigue rated for 3000 psi working pressure while their burst pressure is rated at 12,000 psi. Since they normally operate at 600 psi maximum system pressure, the result is an overall design safety factor of 20 based on ultimate pressure.

Upon completion of assembly and hydraulic tests, all hydraulic subassemblies of the RMS were subjected to a proof pressure test of 1.5 times the system pressure. This pressure was applied and held for five minutes for all internal circuits and vessels of each subassembly which operate at system pressure.

It is important to remember that after a hydraulic failure has occurred and all motion has stopped, the significant remaining hazard is the possibility of injury related to slipping on an oily surface.

5.4.2.4 ELECTRICAL FAILURES RELATING TO THE HEXAPOD

If the sump pump unit fails to pump oil out of the reservoir, a flood level switch which detects reservoir oil level above the normal high level sensor is provided as an input to the controller. A software limit can be programmed to notify the operator and/or shutdown the system.

5.4.3 HYDRAULIC SUPPLY AND DISTRIBUTION SAFETY ANALYSIS

5.4.3.1 HYDRAULIC SUBSYSTEM DESCRIPTION

The hydraulic supply and distribution subsystem is composed of the following components:

- hydraulic power unit (HPU)
- hydraulic service manifold (HSM)
- hydraulic distribution manifolds

Each of these components are described in detail below. To aid in understanding overall system and subsystem functionality, refer to MTS Hydraulic Schematic - Ride Motion Simulator (MTS part number 527212-01).

<u>Hydraulic Power Unit</u>

The hydraulic power unit (HPU) is the source of hydraulic power to the RMS actuators. The HPU is capable of delivering up to 200 gpm at a pressure of 1200 psi. The HPU is located in a separate room from the RMS and supplies hydraulic power to the RMS via pressure, return and drain piping. The piping is sized to limit the pressure drop between the HPU and RMS to an acceptable level. The RMS controller monitors HPS status and controls the operating mode of the HPS. Hydraulic Power On and Off are the principal operating modes and are controlled by RMS electronics and software.

Safety Features

- All high pressure components are designed for 3000 psi of continuous pressure with a minimum safety factor of 4 (12,000 psi burst) and the pumps are rated for 5000 psi. An actual operating pressure of 600 psi allows for a safety factor of at least 20.

- An over-temperature switch and a low-level switch protect the system from abnormal operating conditions. Shutdown of the HPU is delayed 2 seconds to give advanced warning to remote control devices.

- The main pressure piping is rated to 5000 psi for continuous pressure with a minimum 4:1 safety factor (20,000 psi burst). Operation of the system at 600 psi allows for a safety factor of approximately 16.

Hydraulic Service Manifold

The hydraulic service manifold (HSM) is located in a trench next to the RMS. It provides for local control of the main hydraulic power supply to the RMS while also providing filtration features. The HSM is also the location where hydraulic power from the HPU is divided into pilot pressure and main pressure sources for the RMS. Pilot pressure provides hydraulic power to actuator safety functions and pilot servovalves and cannot be interrupted by the HSM controls. Pilot pressure is always ON whenever the HPU is ON. The main source of hydraulic pressure to the RMS which enables motion is controlled at the HSM and there are three operational states: OFF, LOW, and HIGH pressure. In the HSM OFF state, only pilot pressure is supplied to the RMS. In the HSM LOW state, the main source of hydraulic pressure to the RMS is regulated to 200 psi. In the HSM HIGH state, the main source of hydraulic pressure to the RMS is regulated to 600 psi. The HSM is connected to the HPU and hydraulic distribution manifolds via hydraulic piping and hose and to the RMS controller via electrical control cables. Note, the HSM only enables the system main hydraulic supply to reach the actuator control manifolds. Platform motion is not possible until safety features built into actuator control manifolds are disengaged.

Safety Features

- the HSM inherently increases system safety since it provides a means of isolating the main source of hydraulic power from the actuator
- a separate pilot supply increases servovalve stability and predictability during system startup and shutdown
- a separate pilot supply ensures safety functions can be engaged before main pressure is turned on
- the ability to operate the system at LOW HSM pressure setting (200 psi) with a low maximum velocity
- operating the simulator at LOW HSM pressure setting (200 psi) greatly reduces the maximum platform velocity making it possible to more safely test and evaluate new simulator features and configurations
- HSM filtration increases system safety since it protects hydraulic control elements from damaging particles
- when the HSM is switched to LOW or OFF the HSM dumps downstream pressure including pressure stored in the main pressure accumulators
- an hydraulic pressure switch installed on the HSM and set at 1400 psi will detect if the supply pressure has been increased; since increased supply pressure will increase the simulator acceleration and velocity capability, controller software limits are configured to prohibit simulator operation if this switch is triggered

Hydraulic Distribution Manifolds

Three hydraulic distribution manifolds located directly below the RMS distribute hydraulic power to the six hexapod actuators. The principle feature of the distribution system is storage of hydraulic energy through the use of accumulators. Each distribution manifold incorporates four main supply pressure accumulators, two main return pressure accumulators, one pilot pressure accumulator, and one abort/retract pressure accumulator. With the exception of the abort/retract function, all accumulators act inline with their respective sources to smooth out pressure peaks or valleys resulting from varying flow demand.

Safety Features

- The abort/retract accumulator and associated controls maintain an isolated volume of pressurized oil which will gently move the simulator into the park position immediately following an E-stop. The function is entirely passive, no electronics or control signals are required other than to initiate the loss of pressure at the main supply pressure via E-stop, HSM or HPU shutdown. The abort/retract accumulators will fully discharge through the actuator control manifolds regardless of initial actuator position.

- Pilot pressure supply to the pilot pressure accumulator is checked upstream at the HSM outlet. This design provides the actuator pilot stage servovalves and safety valves with a limited supply of oil in the event the HSM or HPU output pressure is lost.

5.4.3.2 HYDRAULIC FAILURES

Hydraulic failures include hydraulic hose failure, loss of hydraulic power, an increase in hydraulic pressure, and hydraulic oil problems.

To mitigate the risk of hydraulic hose failure, RMS supply pressure hoses are rated for 3000 psi working pressure. Since the burst pressure of these hoses is 12,000 psi, a design safety factor of four, based on ultimate, is inherent in the hose working pressure rating. Since the RMS system pressure is 600 psi, this increases the inherent design safety factor of hoses by 5 times, raising the overall safety factor of RMS pressure hoses to 20. A parallel argument can be made regarding hydraulic fittings used on the RMS.

The RMS controller monitors HPS status and controls the operating mode of the HPS. The controller will shut down the system if abnormal hydraulic conditions occur.

- Unexpected loss of hydraulic power will cause the controller to shutdown the system.

- An over-temperature switch and a low-level switch protect the system from abnormal operating conditions. These signals feedback to software limit detectors.

- A hydraulic pressure switch installed on the HSM and set at 1400 psi will detect if the supply pressure has been increased; since increased supply pressure will increase the simulator acceleration and velocity capability, controller software limits are configured to prohibit simulator operation if this switch is triggered.

- Pilot pressure supply to the pilot pressure accumulator is checked upstream at the HSM outlet. This design provides the actuator pilot stage servovalves and safety valves with a limited supply of oil in the event the HSM or HPU output pressure is lost.

5.4.4 ELECTRONIC CONTROLS SAFETY ANALYSIS

5.4.4.1 ELECTRONIC CONTROL DESCRIPTION

The electrical control has two parts; the Operator Interface and the Real-Time Controller console. The Operator Interface is connected to the Real-Time Controller via thin-wire ethernet. The Real-Time Controller connects with the system actuators, transducers and detectors through cables protected by conduit. Both parts of the electrical control derive their power from an uninterruptable power supply (Government supplied) to protect them from incoming line surges, spikes, brownouts and blackouts.

5.4.4.2 TRANSDUCER FAILURES

All electrical transducers located in the pit are of industrial quality and benefit from the regulations governing the safety of such equipment. The equipment functions normally even when wet with oil. The low operating temperature of the working fluid and its low volatility lessen the fire hazard.

If a transducer fails, the Real-Time Controller will react to a position or acceleration software limit. The controller will then proceed with an E-Stop procedure. With regular maintenance, calibration, safety startups and dynamic pretests the likelihood of a transducer fault is minimal.

5.4.4.3 REAL-TIME CONTROLLER ELECTRICAL FAILURES

The Real-Time Controller consists of a VME computer, digital and analog signal conditioning and various low voltage power supplies.

The VME computer is made up of several circuit cards. The processor card is a Motorola 2604 processor that runs at 200MHz with 16 MB RAM. The other interface cards are designed and manufactured by MTS. They include A/D and D/A converters, digital I/O channel interface and Temposonic III interface. All of the VME cards are manufactured to their applicable standards and are utilized on hundreds of other industrial projects throughout the world.

The signal conditioning interface is manufactured by MTS. There are several different types of conditioning used on this system. All of the signal conditioning cards are manufactured to their applicable standards and are utilized on hundreds of other industrial projects throughout the world.

The power supplies provide power to the signal conditioners (and therefore transducers) within this system. The power supply voltages to the signal conditioners are continuously monitored to stay above safe minimum limits.

Since all components are manufactured for use in industrial environments, the chance of individual failure is minimal. Since failures can occur, and we must control the manner in which the system reacts to all possible errors, the software and hardware is designed to continuously monitor all signals.

There are two basic methods employed to mitigate error or failures within the system. The first is the constant monitoring of all input channels. This includes comparing the incoming signal to predefined min/max absolute limits and min/max error limits (both position and acceleration). This software monitoring can initiate either a controlled shutdown of the system or a Emergency Stop (E-Stop) shutdown. The second method is a hardwired E-Stop chain which monitors the consent switches, watchdog timers, and several E-Stop buttons. The E-Stop chain will initiate a mechanical protection reaction to bleed down the actuator pressure without exerting undue forces to the occupant of the simulator.

Control console fire is a possibility; however it is minimized by using only industrial rated devices operating within their rated capacity. Further, the installation of the control console equipment is carried out in accordance with best practice. In the event a fire should occur in the console or the pit area, manually operated fire extinguishers rated for Class A and Class B & C should be within 10 feet of the console.

5.4.4.4 OPERATOR INTERFACE ELECTRICAL FAILURE

The Operator Interface consists of a IBM compatible Pentium 450 MHz computer with a 21" monitor, keyboard and mouse. The user utilizes a custom interactive program to define, select, start and stop a program on the simulator. If proper defining and selecting procedures are followed, the chance of an extreme motion of the occupant is remote.

The computer's operating system is Microsoft Windows NT 4.0. This operating system offers the most protection available for personal computers from a system freeze error. If the system encounters a power failure or a system freeze error, the Real-Time Controller will notice a lack of communication over the Ethernet link and shut the system down accordingly. Since the program defining the motions of the system reside on the Real-Time Controller, the system will not have any uncontrolled motion as a result of a system error on the Operator Interface Computer.

5.4.5 CONTROLLER SOFTWARE SAFETY ANALYSIS

Meeting the specified performance targets, particularly for high-bandwidth vibration performance, requires the use of a sophisticated and complex control system with many performance optimizing adjustments. Because feedback techniques are employed, unstable conditions are possible that may not be immediately apparent to the operator. When the control system is unstable, uncontrollable and violent high frequency oscillations are the normal and expected behavior of the system. This property, combined with the power and bandwidth of the hydraulics, can lead to high velocities and accelerations.

The platform and payload together define a complex and non-linear system. The payload itself is a part of the control loop and may contain elements that can negatively affect the stability of the controller. Because the operator may introduce new payloads as a part of normal system operation, the issue of controller tuning, system stability and safety require ongoing attention.

It is the responsibility of the operator to insure that controller feedback loops and related adjustments are configured safely and that the payload is itself sufficiently stable to permit controllability under all foreseen conditions. There are inherent trade-offs between controller performance (bandwidth and tracking) and the safety of the system that must be addressed by a properly trained operator familiar with feedback control theory and its practical application to this system.

5.4.5.1 CONTROLLER SOFTWARE SAFETY FEATURES

The software system contains many safety features to mitigate danger to the crew. Some of these safety features are automatic and redundant. Others require careful configuration by an operator extensively trained in human factors engineering. Especially important are detailed understanding of human physiological limits to shock and vibration. These limits have complex magnitude, duration and frequency properties that must be understood to reduce the probability of immediate or cumulative injuries to the crew.

The following software safety features are provided:

- Feedback vs Feedforward Control

  The controller features an inverse dynamics-based feedforward control strategy. This technique attempts to forecast the required valve openings to follow the command trajectory. When properly configured with settings that match the physical description of the payload, it enables the system to achieve reasonable performance without using high gain settings in the feedback controller. This feature can improve the safety of the crew by reducing the probability of instability in the controller.

- Access Levels

  Three access levels are defined for the system: Basic, Service and Extended. The Service and Extended access levels are protected by distinct passwords.

  The Basic level allows operation of the platform and access to all the diagnostic features. The Basic operator may start the system, move the platform with the manual controls or function generators and play back pre-recorded motion files. The Basic operator may also configure the platform for external control by the vehicle dynamics subsystem during a simulation.

  The Service access level enables system calibration and tuning features. The Service operator can use the calibration menu panels and controller tuning panels to adjust control system performance.

  The Extended access level is for software developers who intend to modify the controller software. The Extended operator may access the interactive programming tools and modify the control system and operator interface panels. Because these features can operate on a running controller, it is imperative that human subjects never occupy the cab when the controller is open to this access level.

  If customer initiated changes are made at the Extended level, the entire safety rating policy for the system must be reviewed.

- Signal Limit Detection

  Software limit detectors monitor many safety-related signals. Each limit detector monitors one signal and compares the value to preset limits. The minimum, maximum and time settings for each limit must be configured by the operator to insure compliance with human subject tolerances. Each limit detector may be configured by the operator to take direct action in the controller when the associated signal is out of bounds:

  - Display : Light the lamp while the signal is TRUE
  - Latch : Latch the value until reset. (Lamp stays on)
  - Hold : Smoothly stop the platform command signal
  - E-Stop : Stop the system and shut down.

  Limits can be set for motion control processor signals, including actuator motion and all command and feedback signals. Limits can also be set for system functions such as oil temperature, oil level, pressure level access ramp down, etc.

- Hardwired Emergency Events

  A digital (discrete logic) input signal is monitored for each of the following event groups:

Crew E-stop	The red button in the crew station
Facility E-stop	The red button on the wall beside the access platform
Facility E-stop	The red button in the pit on the guard rail
Console E-stop	The red button on the control console desk
497 failure	Self-detected error inside 497 conditioner box
497 No. 1 power failure	Power failure to 497 number 1
497 No. 2 power failure	Power failure to 497 number 2

  This group of signals is always configured to shutdown (E-stop) the system. The software displays and logs these events.

- Message Logging

  The Message Log panel displays a text message for each occurrence of a significant controller event. Each entry to the log has a date, time and message text that describes the event. Messages are logged for all control. Significant events include all controller state changes, calibration alterations and the occurrence of and limit detector events configured by the operator.

- Processor Watchdogs

  Three processors operate the control system: the host workstation and two digital signal processors. Each DSP generates a signal which is monitored by an external hardware watchdog circuit. If either processor fails to maintain this signal, an automatic emergency shutdown occurs.

In addition, Table 5-1 lists RMS failures and effects that were demonstrated to TARDEC's Safety Office before it could pass a safety release for man-rating.

Ride Motion Simulator
Failure and Effect Table

Failure/Switch	Effect on RMS	Action Taken	Verified
Emergency stop button in pump room	Software reads pump is off, simulator loses pressure, E-stop is initiated.	Operator can restart normally, once pump is reset.	
High to low pressure change in pump room	Servo error detected in Z (interlock triggered), simulator safely shuts down.	Operator has to reset error to start over.	
Simulate MTS 498 controller power loss	Simulator experiences a jerk, E-stop is initiated and simulator shuts down.	Operator should quit controller application before restarting console.	
Simulate MTS 497 chassis power loss	Simulator experiences a small jerk, E-stop is initiated and simulator shuts	Operator should restore power to the 497 and restart the application.	
Simulate power loss to interface (PC on console)	Monitor screen goes blank, simulator has a tamed stop and stays at operating	Restart by hitting E-stop button.	
Simulate operator error on monitor (i.e. close window)	Not possible to close window, if selecting "quit" (prompts you to turn	Use red E-stop immediately for cases like Windows NT crashing	
Emergency stop button on console	Simulator experiences no jerks and safely shuts down automatically.	Reset E-stops and start simulator up again.	
Emergency stop button in cab	Simulator experiences no jerks and safely shuts down automatically.	Reset E-stops and start simulator up again.	
Emergency stop button #1 in pit	Simulator experiences no jerks and safely shuts down automatically.	Reset E-stops and start simulator up again.	
Emergency stop button #2 in pit	Simulator experiences no jerks and safely shuts down automatically.	Reset E-stops and start simulator up again.	
Reset button on hydraulic pump	No effect on simulator.	No action needed.	

Table 5-1. Failures and Effects

Ride Motion Simulator
Failure and Effect Table

Failure/Switch	Effect on RMS	Action Taken	Verified
UPS input voltage lost (Uninterruptible Power Supply)	No effect on UPS because batteries act as power back-up.	Bring simulator down, turn hydraulic manifolds off before restoring power.	
Simulate power failure to digital I/O	E-stop initiated. Simulator shuts down safely.	Does not effect software, can begin simulation again by starting simulator.	
Simulate power failure to analog I/O	E-stop initiated. Simulator shuts down safely.	Does not effect software, can begin simulation again by starting simulator.	
Simulate power failure to Temposonics III card	E-stop initiated. Simulator shuts down safely.	Does not effect software, can begin simulation again by starting simulator.	
Simulate Ethernet failure to MTS 498 Controller	Timer set conservatively to shutdown simulator automatically, receive socket	Hit E-stop, restart software application as with any PC problems.	
Test Motion Consent Switch on console (local	Turning key from local to remote acts as an E-stop, simulator safely shuts down.	Return key switch to proper position and restart simulator.	
Test Motion Consent Switch in cab (yes to no	Turning key from yes to no acts as an E-stop, clear E-stops before starting	Return key switch to proper position and restart simulator.	
Position command input exceeded	Limit is detected, E-stop initiated and simulator safely shuts down.	Reset E-stop and restart simulator.	
Rate command input limit exceeded	Limit is detected, E-stop initiated and simulator safely shuts down.	Reset E-stop and restart simulator.	
Acceleration command input limit exceeded	Limit is detected, E-stop initiated and simulator safely shuts down.	Reset E-stop and restart simulator.	
Simulate loss of power to sump pump	No effect on simulator.	Restore power ASAP to avoid overflow of oil into the pit otherwise turn pump off.	

Table 5-1. Failures and Effects (continued)

Ride Motion Simulator
Failure and Effect Table

Failure/Switch	Effect on RMS	Action Taken	Verified
Position limit exceeded (feedback)	Motion stops abruptly and E-stop is initiated.	Reset E-stop and restart simulator.	
Rate limit exceeded (feedback)	Motion stops abruptly and E-stop is initiated.	Reset E-stop and restart simulator.	
Acceleration limit exceeded (feedback)	Motion stops abruptly and E-stop is initiated.	Reset E-stop and restart simulator.	

Table 5-1. Failures and Effects (continued)

5.4.5.2 SAFETY PROCESSOR

One of the DSP processors has extra safety functions; all simulation commands enter this processor directly from the SCRAMNet and are monitored by a set of limit detectors. The simulation command signals specify the desired X, Y, Z accelerations and three rotational rates for the cab. Each of these signals has an associated limit with bounds configurable by the operator. This group of signals is then processed by the washout filters to create the actual motion commands sent to the controller on the other DSP. The motion commands from the washout filters are monitored by another set of limits before being sent to the motion controller.

The safety processor also monitors a watchdog signal from the motion controller processor and sends this value to the hardware watchdog circuit. If the motion controller or safety processor fail to propagate this signal, the hardware will shutdown hydraulic power to the platform.

Since most of the complex software runs on the motion control processor, the safety processor is less vulnerable to failure due to programming flaws and is expected to report a total failure (crash) in the motion controller software.

5.4.5.3 SAFETY DIAGNOSTIC TOOLS

Because of the paramount importance of controller stability, some specialized tools associated with controller optimization are also valuable for safety assessment. The Transfer Function Estimator may be used in conjunction with the Frequency Response Plotter to display the gain and phase characteristics of the controller payload system. Proper assessment of this plot can help the operator establish a safer compromise between performance and stability.

5.5 SYSTEM HAZARD ANALYSIS TABLE

The accompanying analysis sheets contain hazard severity levels and hazard probability levels from MIL-STD-882C. These hazard levels allow system damage and personal injury to be included in the definition and reflected in the hazard assessment.

HAZARD SEVERITY LEVELS

a. Category I - Catastrophic. May cause death or system loss.

b. Category II - Critical. May cause severe injury, severe occupational illness, or major system damage.

c. Category III - Marginal. May cause minor injury, minor occupational illness, or minor system damage.

d. Category IV - Negligible. Will not result in injury, occupational illness, or system damage.

HAZARD PROBABILITY LEVELS

A - Likely to occur immediately

B - Probably will occur in time

C - Possible to occur in time

D - Unlikely to occur in time

SYSTEM HAZARD ANALYSIS TABLE

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Impact/Crushing Physical Injury	Structural failure of hexapod platform, swivels, actuators, reaction base	Possible severe damage to the RMS depending on the locations and severity of structural damage	II	D	Since a hexapod mechanism becomes unconstrained if one actuator is removed, the worst case hazard is that an actuator completely breaks away at one end and the remaining structure topples over. If such an event would occur, multiple controller limits would be violated thus triggering emergency shutdown. To mitigate this hazard, major load carrying elements of the RMS were designed with: a minimum safety factor of 4, redundant load paths whenever possible, and conservative limit load specifications for each degree-of-freedom. Mandatory use of seat belts during any motion of system should be enforced. Following the maintenance schedule and a pre-test checklist will greatly reduce the possibility of this type of hazard.
	Structural failure of cab structure or components	Possible damage to the RMS, possible severe damage to the cab	II	D	Critical cab structure elements concerning human safety are the seat support and the monitor support. Failure of these elements could result in structural members impacting the test subject. To mitigate this hazard, cab structural elements were designed with: a minimum safety factor of 4, redundant load paths whenever possible, and conservative limit load specifications for each degree-of-freedom. Following the maintenance schedule and a pre-test checklist will greatly reduce the possibility of this type of hazard.
	Person entering pit area during test run	Possible physical injury to person	II	D	Access to pit area limited to experience maintenance personnel. All personnel should have proper training before entering pit area.

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Electrical shock	Wear or severing of power cables to actuator drain sump pump and actuator solenoids	Electrical shock to personnel	II	D	Design is based on industry standards National Electrical Code. Actuator drain sump pump voltage (460 V) is conduit enclosed per National Electrical code. Solenoid voltage (24 Vdc) is not a hazard.

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Chemical Exposure	Burst in hose or rupture in manifold resulting in large scale oil leakage	Power to the RMS will end, release of hydraulic oil into room	IV	D	The exact location of the failure and the equipment wetted by the escaping oil determines the severity of the hazard. The hazard to personnel varies with the amount and velocity of oil delivered and point of impact. Burn hazard is non-existent based on the maximum oil temperature being limited to 140°F. Immediate control of the hazard depends on system shutdown by the operator or controller limits. Using an industry standard petroleum based hydraulic fluid (refer to the MSDS for Mobil DTE25 in Appendix A). A good preventative maintenance program and periodic inspection of equipment keeps the probability of occurrence remote.

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Fire and Smoke Exposure	Ignition of oil from spark or open flame	Possible severe damage depending on the extensiveness of the fire	II	D	Using an industry standard petroleum based hydraulic fluid (refer to the MSDS for Mobil DTE25 in Appendix A). It is highly unlikely that the hydraulic fluid could burn since it has a flash point of 395°F. However, pressurized oil from a leak or spray has a greater probability of combustion if it comes into contact with a flame or spark. The main pump motor is of drip-proof construction. Banning any open flames or smoking materials from the area will reduce the chance of fire to almost zero.

SYSTEM HAZARD ANALYSIS TABLE (con't)

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Sustained Physical Acceleration	Hardware or software failure or setup error which causes control instability	high acceleration and deceleration possible over a broad band of frequency before controller invokes shutdown	III	D	Worst case scenario implies sinusoidal motion at the performance limits of the machine. Multiple feedback parameter out-of-bound conditions will be detected by controller limits thus triggering emergency shutdown. Pressure relief valves and hydraulic cushions prevent damage to machine. Resulting acceleration/deceleration vector unpredictable therefore human injury from flailing limbs, head or body resonance also unpredictable. The RMS operator can stop the test by pressing the "Red" master stop button, or the test subject can activate the E-stop button in the cab. Following the maintenance schedule and a pre-test checklist will reduce the possibility of this type of failure.
	Limit detectors disabled	large acceleration, velocity, and displacements are possible over a broad band of frequency	III	D	The operator cannot change the status of the limit detectors. If limit detectors are disabled, controller triggered emergency shutdown will not occur and the machine will follow the motion commands to the extent of performance limits. Worst case scenario #1 implies maximum acceleration and velocity followed by maximum deceleration at actuator extreme positions (position commands go outside of machine displacement limits). Worst case scenario #2 implies random or periodic motion imparting sustained maximum acceleration/deceleration to the test subject (position commands remain within bounds of machine displacement limits). Following a pre-test checklist will reduce the possibility of limit detectors being disabled.

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
High Physical Acceleration	Loss of controller hardware, servo-valve failure, valve driver failure, feedback transducer, cable, or conditioner failure	high acceleration possible before complete shutdown	III	C	Worst case scenario implies high velocity near displacement limits concurrent with controller loss; established kinetic energy and trajectory could result in multiple actuator cushion impact before controller shutdown can arrest motion. Pressure relief valves and hydraulic cushions prevent damage to machine. Resulting acceleration/deceleration vector unpredictable therefore human injury from flailing limbs or head also unpredictable. The RMS operator can stop the test by pressing the "Red" master stop button, or the test subject can activate the E-stop button in the cab. Following the maintenance schedule and a pre-test checklist will reduce the possibility of this type of failure.

SYSTEM HAZARD ANALYSIS TABLE (con't)

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
High Physical Acceleration (con't)					
	Data file error	high acceleration and deceleration possible before controller invokes shutdown	III	D	Worst case scenario implies high velocity through set displacement limits; established kinetic energy and trajectory could result in multiple actuator cushion impact before controller shutdown can arrest motion. Most likely system will shutdown fast enough, but this is not guaranteed. Pressure relief valves and hydraulic cushions prevent damage to machine. Resulting acceleration/deceleration vector unpredictable therefore human injury from flailing limbs or head also unpredictable. Data to be simulated should be generated from well proven analytical models. Additionally, all data should be visually inspected and a simulation executed without the test subject in the RMS. The RMS operator can stop the test by pressing the "Red" master stop button, or the test subject can activate the E-stop button in the cab. Following the maintenance schedule and a pre-test checklist will reduce the possibility of this type of failure.
	Loss of integrity of external input signal to RMS	Invalid signals sent to the RMS from external device	III	D	All output data is filtered using the electronic filters which would smooth over any sudden changes in signal. Invalid signals should be detected in the testing phase before the test subject has boarded the simulator.
	Incorrect electrical connections	Undesirable movement of the simulator. Loss of control.	III	D	Changing the RMS motion electrical connections is unlikely. Pre-simulation testing will reveal incorrect settings of the control modules or incorrect hookups of the input signal. Corrections will then be made. Also, a preliminary dry run each morning will greatly reduce the possibility of this type of hazard.
	Operator or occupant errors resulting in failure to stop test, perhaps placing occupant in a dangerous situation	Failure to stop test	III	C	Failure of either the operator or occupant to stop a test and cause possible damage to the occupant (and equipment) is prevented by providing both people the ability to stop a test. If neither person acts to stop a test, additional safety is provided through automatic shutdown (servo controller limits) which will stop a test when travel limits have been exceeded.

SYSTEM HAZARD ANALYSIS TABLE (con't)

HAZARD	CAUSES	EFFECTS	HAZARD SEVERITY	HAZARD PROBABILITY	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Minimal.	Failure of UPS system	Fluctuations in electrical supply power to the RMS	N.A.	D	The UPS (Uninterruptible Power Supply) system will provide power to the entire RMS electrical system. The UPS will regulate voltage, frequency, and remove noise from the input line voltage. It will also provide power if the input line voltage is lost. The UPS guarantees a clean and continuous power supply to the RMS and associated equipment. Failure of the UPS system in itself poses no problem because unregulated line voltage will be available.
	Loss of input line voltage to RMS control electronics and hydraulic pump	Loss of electrical power to RMS control electronics and hydraulic pump	N.A.	C	The UPS system will provide power to the entire RMS electrical system except for the hydraulics. The UPS will provide power for up to 15 minutes if the input line voltage is lost. The UPS guarantees a clean and continuous electrical power supply to the RMS. The hydraulic pump will lose power but the accumulator's discharge will smooth loss of performance at the machine. Eventually feedback parameter out-of-bounds conditions will be detected by controller limits thus triggering emergency shutdown.
	Noise on the power lines (perhaps due to electrical storm)	Input line voltage is no longer at 115 VAC	N.A.	C	The UPS system protects all RMS control electronics from voltage surges except the hydraulic pump. Hydraulic pump motors are insensitive to short duration voltage surges although voltage spikes could result in current spikes which could trip the breakers. Loss of 3-phase power to the hydraulic pump will result in loss of pressure to the RMS, resulting in an E-stop condition.
	Loss of Hydraulic Pressure	Hydraulic power to the RMS decreases or stops	N.A.	D	Loss of system pressure due to loss of pump power, blockage in lines, clogged hydraulic filters, burst in hose or fitting, component failure, etc. implies a decrease in flow volume and hence a rapid decrease in machine performance. The accumulator's discharge will smooth the loss of performance. Eventually feedback parameter out-of-bound conditions will be detected by controller limits thus triggering emergency shutdown. A good preventative maintenance program and periodic inspection of equipment keeps the probability of occurrence remote.
	Hydraulic Pressure Fluctuations	Varying output pressure of hydraulic pump, instead of constant	N.A.	D	HPS pressure controls have a variation of 100-200 psi when controlling to any specific set pressure. Pressure surges and dips can also occur due to many factors: hard-line pressure drop, water hammer, oil separation, pressure control valve dynamic response to changes in required flow, etc. Short duration pressure pulses are dampened by the accumulators. Sudden sustained low pressure would indicate a large leak. Sustained high pressure would indicate a relief valve malfunction. A pressure compensated pump is designed to de-stroke in the face of increased pressure, eventually going to near zero. Pump pressure compensators are quick acting (<100 msec) to limit over and under-pressure surges. A sustained pressure surge to the actuators is only possible by simultaneous failure of the pump relief valve, compensator and pressure switch. A pressure surge does not in itself define an injury situation. Following the maintenance schedule and a pre-test checklist will greatly reduce the possibility of this type of situation.

(This page has been intentionally left blank)

APPENDIX A

MATERIAL SAFETY DATA SHEETS

Mobil

MOBIL OIL CORPORATION MATERIAL SAFETY DATA BULLETIN

REVISED:09/24/91

********************** I. PRODUCT IDENTIFICATION **********************

MOBIL DTE 25

SUPPLIER:
MOBIL OIL CORP.
CHEMICAL NAMES AND SYNONYMS:
PET. HYDROCARBONS AND ADDITIVES
USE OR DESCRIPTION:
HYDRAULIC OIL

24-HOUR EMERGENCY (CALL COLLECT):
(609) 737-4411
CHEMTREC:
(800) 424-9300
PRODUCT AND MSDS INFORMATION:
(800) 662-4525

************ II. TYPICAL CHEMICAL AND PHYSICAL PROPERTIES ************

APPEARANCE: Dark Amber Liquid ODOR: Mild PH: NA
VISCOSITY AT 100 F, SUS: 238.0 AT 40 C, CS: 46.0
VISCOSITY AT 210 F, SUS: 48.0 AT 100 C, CS: 7.0
FLASH POINT F(C): > 395(202) (ASTM D-92)
MELTING POINT F(C): NA POUR POINT F(C): -10(-23)
BOILING POINT F(C): > 600(316)
RELATIVE DENSITY, 15/4 C: 0.885 SOLUBILITY IN WATER: Negligible
VAPOR PRESSURE-mm Hg 20C: < .1

NA=Not Applicable NE=Not Established D=Decomposes
FOR FURTHER INFORMATION, CONTACT YOUR LOCAL MARKETING OFFICE.

**************** III. POTENTIALLY HAZARDOUS INGREDIENTS ***************

None

SEE SECTIONS XII AND XIII FOR REGULATORY AND FURTHER COMPOSITIONAL DATA.

SOURCES: A=ACGIH-TLV, A*=Suggested-TLV, M=Mobil, O=OSHA, S=Supplier
NOTE: Limits shown for guidance only. Follow applicable regulations.

*********************** IV. HEALTH HAZARD DATA ***********************

--- INCLUDES AGGRAVATED MEDICAL CONDITIONS, IF ESTABLISHED ---
THRESHOLD LIMIT VALUE: 5.00 mg/m3 Suggested for Oil Mist
EFFECTS OF OVEREXPOSURE: Not expected to be a problem.

*************** V. EMERGENCY AND FIRST AID PROCEDURES ****************

--- FOR PRIMARY ROUTES OF ENTRY ---
EYE CONTACT: Flush thoroughly with water. If irritation persists, call a physician.
SKIN CONTACT: Wash contact areas with soap and water. High pressure accidental injection through the skin requires immediate medical attention for possible incision, irrigation and/or debridement.
INHALATION: Not expected to be a problem.
INGESTION: Not expected to be a problem. However, if greater than 1/2 liter(pint) ingested, immediately give 1 to 2 glasses of water and call a physician, hospital emergency room or poison control center for assistance. Do not induce vomiting or give anything by mouth to an unconscious person.

****************** VI. FIRE AND EXPLOSION HAZARD DATA ******************

FLASH POINT F(C): > 395(202) (ASTM D-92)
FLAMMABLE LIMITS. LEL: .6% UEL: 7.0%
EXTINGUISHING MEDIA: Carbon dioxide, foam, dry chemical and water fog.
SPECIAL FIRE FIGHTING PROCEDURES: Water or foam may cause frothing. Use water to keep fire exposed containers cool. Water spray may be used to flush spills away from exposure. For fires in enclosed areas, firefighters must use self-contained breathing apparatus. Prevent runoff from fire control or dilution from entering streams, sewers, or drinking water supply.
UNUSUAL FIRE AND EXPLOSION HAZARDS: None.
NFPA HAZARD ID: Health: 0, Flammability: 1, Reactivity: 0

************************* VII. REACTIVITY DATA *************************

STABILITY (Thermal, Light, etc.): Stable
CONDITIONS TO AVOID: Extreme heat.
INCOMPATIBILITY (Materials to Avoid): Strong oxidizers
HAZARDOUS DECOMPOSITION PRODUCTS: Carbon monoxide.
HAZARDOUS POLYMERIZATION: Will not occur.

********************* VIII. SPILL OR LEAK PROCEDURE *******************

ENVIRONMENTAL IMPACT: Report spills as required to appropriate authorities. U. S. Coast Guard regulations require immediate reporting of spills that could reach any waterway including intermittent dry creeks. Report spill to Coast Guard toll free number (800) 424-8802. In case of accident or road spill notify CHEMTREC (800) 424-9300.
PROCEDURES IF MATERIAL IS RELEASED OR SPILLED: Adsorb on fire retardant treated sawdust, diatomaceous earth, etc. Shovel up and dispose of at an appropriate waste disposal facility in accordance with current applicable laws and regulations, and product characteristics at time of disposal.
WASTE MANAGEMENT: Product is suitable for burning in an enclosed, controlled burner for fuel value or disposal by supervised incineration. Such burning may be limited pursuant to the Resource Conservation and Recovery Act. In addition, the product is suitable for processing by an approved recycling facility or can be disposed of at any government approved waste disposal facility. Use of these methods is subject to user compliance with applicable laws and regulations and consideration of product characteristics at time of disposal.

***************** IX. SPECIAL PROTECTION INFORMATION ******************

EYE PROTECTION: No special equipment required.
SKIN PROTECTION: No special equipment required. However, good personal hygiene practices should always be followed.
RESPIRATORY PROTECTION: No special requirements under ordinary conditions of use and with adequate ventilation.
VENTILATION: No special requirements under ordinary conditions of use and with adequate ventilation.

*********************** X. SPECIAL PRECAUTIONS ************************

No special precautions required.

*********************** XI. TOXICOLOGICAL DATA ************************

---ACUTE TOXICOLOGY---

ORAL TOXICITY (RATS): Slightly toxic ---Based on testing of similar products and/or the components.

DERMAL TOXICITY (RABBITS): Slightly toxic ---Based on testing of similar products and/or the components.

INHALATION TOXICITY (RATS): Not applicable ---Harmful concentrations of mists and/or vapors are unlikely to be encountered through any customary or reasonably foreseeable handling, use, or misuse of this product.

EYE IRRITATION (RABBITS): Expected to be non-irritating. ---Based on testing of similar products and/or the components.

SKIN IRRITATION (RABBITS): Expected to be non-irritating. ---Based on testing of similar products and/or the components.

---SUBCHRONIC TOXICOLOGY (SUMMARY)---

Severely solvent refined and severely hydrotreated mineral base oils have been tested at Mobil Environmental and Health Sciences Laboratory by dermal application to rats 5 days/week for 90 days at doses significantly higher than those expected during normal industrial exposure. Extensive evaluations including microscopic examination of internal organs and clinical chemistry of body fluids, showed no adverse effects.

---CHRONIC TOXICOLOGY (SUMMARY)---

The base oils in this product are severely solvent refined and/or severely hydrotreated. Chronic mouse skin painting studies of similar oils showed no evidence of carcinogenic effects.

********************* XII. REGULATORY INFORMATION *********************

GOVERNMENTAL INVENTORY STATUS: All components registered in accordance with TSCA and EINECS.

DOT:

Shipping Name: Not applicable
Hazard Class: Not applicable

US OSHA HAZARD COMMUNICATION STANDARD: Product assessed in accordance with OSHA 29 CFR 1910.1200 and determined not to be hazardous.

RCRA INFORMATION: The unused product, in our opinion, is not specifically listed by the EPA as a hazardous waste (40 CFR, Part 261D); does not exhibit the hazardous characteristics of ignitability, corrosivity, or reactivity, and is not formulated with the contaminants listed in the Toxicity Characteristic (TC) Rule as determined by the Toxicity Characteristic Leaching Procedure (TCLP). However, used product may be regulated.

U.S. Superfund Amendments and Reauthorization Act (SARA) Title III:
This product contains no "EXTREMELY HAZARDOUS SUBSTANCES".

SARA (311/312 - FORMERLY 302) REPORTABLE HAZARD CATEGORIES: None

This product contains no chemicals reportable under SARA (313) toxic release program.

THE FOLLOWING PRODUCT INGREDIENTS ARE CITED ON THE LISTS BELOW:

CHEMICAL NAME	CAS NUMBER	LIST CITATIONS
ZINC (ELEMENTAL ANALYSIS) (.06%)	7440-66-6	15
PHOSPHORODITHOIC ACID, O,O-DI C1-14-ALKYL ESTERS, ZINC SALTS (2:1) (ZDDP) (.67%)	68649-42-3	15

--- KEY TO LIST CITATIONS ---

1 = OSHA Z, 2 = ACGIH, 3 = IARC, 4 = NTP, 5 = NCI,
6 = EPA CARC, 7 = NFPA 49, 8 = NFPA 325M, 9 = DOT HMT, 10 = CA RTK,
11 = IL RTK, 12 = MA RTK, 13 = MN RTK, 14 = NJ RTK, 15 = MI 293,
16 = FL RTK, 17 = PA RTK, 18 = CA P65.

--- NTP, IARC, AND OSHA INCLUDE CARCINOGENIC LISTINGS ---

NOTE: MOBIL PRODUCTS ARE NOT FORMULATED TO CONTAIN PCBS.

************************* XIII. INGREDIENTS *************************

INGREDIENT DESCRIPTION	PERCENT	CAS NUMBER
CONTAINS ONE OR MORE OF THE FOLLOWING BASE OILS:	> 95.00	
DISTILLATES (PETROLEUM), HYDROTREATED HEAVY PARAFFINIC		64742-54-7
DISTILLATES (PETROLEUM), SOLVENT-DEWAXED HEAVY PARAFFINIC		64742-65-0
DISTILLATES (PETROLEUM), HYDROTREATED LIGHT PARAFFINIC	0.18	64742-55-8

Mobil

****************************** APPENDIX **********************************

FOR MOBIL USE ONLY: MCN: , MHC: 1* 1* NA 0* 0*, MPPEC: A, PPEC: A, US91-461 APPROVE 09/17/91 REQ: US - MARKETING

****

INFORMATION GIVEN HEREIN IS OFFERED IN GOOD FAITH AS ACCURATE, BUT WITHOUT GUARANTEE. CONDITIONS OF USE AND SUITABILITY OF THE PRODUCT FOR PARTICULAR USES ARE BEYOND OUR CONTROL; ALL RISKS OF USE OF THE PRODUCT ARE THEREFORE ASSUMED BY THE USER AND WE EXPRESSLY DISCLAIM ALL WARRANTIES OF EVERY KIND AND NATURE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE IN RESPECT TO THE USE OR SUITABILITY OF THE PRODUCT. NOTHING IS INTENDED AS A RECOMMENDATION FOR USES WHICH INFRINGE VALID PATENTS OR AS EXTENDING LICENSE UNDER VALID PATENTS. APPROPRIATE WARNINGS AND SAFE HANDLING PROCEDURES SHOULD BE PROVIDED TO HANDLERS AND USERS.

****

PREPARED BY: MOBIL OIL CORPORATION
ENVIRONMENTAL HEALTH AND SAFETY DEPARTMENT, PRINCETON, NJ

FOR FURTHER INFORMATION, CONTACT:
MOBIL OIL CORPORATION, PRODUCT FORMULATION AND QUALITY CONTROL
3225 GALLOWS ROAD, FAIRFAX, VA 22037 (800) 227-0707 X3265

DISTRIBUTION LIST

Copies

Commander
U.S. Army Tank-automotive and Armaments Command
ATTN: AMSTA-TR (Mr. Chapin) 1
AMSTA-TR-VP (Mr. Adlam) 1
AMSTA-TR-VP (Dr. Beck) 1
AMSTA-TR-VP (Mr. Culling) 1
AMSTA-TR-VP (Bldg 215) 10
AMSTA-CS-CZ (Mr. Kelley) 1
AMSTA-TR-O (Technical Information Center) 2
Warren, MI 48397-5000

Director
U.S. Army Test and Evaluation Command
ATTN: AMSTE-SM-S (Mr. Kietzman) 4
Aberdeen Proving Ground, MD 21005-5055

Commander
Defense Technical Information Center
ATTN: DTIC-BRR 2
8725 John J. Kingman Road, STE 0944
FT. Belvoir, VA 22060-6218

MTS Systems Corporation
ATTN: Mr. Tim Zappia 3
ATTN: Mr. Mark Winslow 1
ATTN: Mr. Hugh Sparks 1
14000 Technology Drive
Eden Prairie, MN 55344

Dynamic Research Incorporated
ATTN: Mr. John Lenkeit 2
355 Van Ness Avenue
Torrance, CA 90501

Dynamics Research Corporation
ATTN: Randy Brooks 5
1755 Jefferson Davis Highway, Suite 802
Arlington, VA 22202